PENDING CLAIMS AS AMENDED

Please amend the claims as follows:

1-63. (Cancelled)

64. (Currently Amended) A method for broadcasting encrypted multimedia content from a content provider to a plurality of authorized terminals over the air, comprising:

each terminal forwarding a unique public key over the air to the content provider, wherein:

each terminal has a mobile equipment and has a secure processing unit that securely stores a unique private key, corresponding to the unique public key, such that the unique private key is not accessible to the mobile equipment of the respective [[a]] terminal ~~user~~,

the secure processing unit provides more secure key storage than the mobile equipment,

the secure processing unit has processing power sufficient to decrypt a broadcast access key and to generate a short term key, and

the secure processing unit does not have processing power sufficient to decrypt multimedia content, and ~~wherein~~

the ~~content provider encrypts a~~ broadcast access key is encrypted by the content provider using ~~with each of~~ the unique public keys of each of the respective terminals to authorize the respective [[a]] terminal ~~having the secure processing unit securely storing a corresponding unique private key~~ to receive ~~the~~ encrypted multimedia content;

each terminal receiving the respective encrypted broadcast access key over the air from the content provider and providing the respective encrypted broadcast access key to the terminal's secure processing unit, wherein the terminal's secure processing unit decrypts the encrypted broadcast access key using the secure processing unit's unique private key and securely stores the broadcast access key;

each terminal receiving short-term key information and encrypted multimedia content broadcast over the air from the content provider to the plurality of terminals, wherein the multimedia content is encrypted with a short-term key, and wherein the short-term key is generated using the broadcast access key and the short-term key information;

each terminal providing the short-term key information to the terminal's secure processing unit, wherein the terminal's secure processing unit generates the short-term key using the broadcast access key and the short-term key information, and provides the short-term key to the terminal's mobile equipment; and

each terminal's mobile equipment decrypting the multimedia content using the short-term key.

65. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 64, wherein the short-term key is accessible to a user.

66. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 65, wherein the short-term key is changed by the content provider at a rate related to a registration cost.

67. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 64, wherein the secure processing unit is removable from the terminal.

68. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 64, wherein the short-term key information is the short-term key encrypted using the broadcast access key.

69. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 64, wherein the short-term key is generated by applying a cryptographic hash to a concatenation of the short-term key information and the broadcast access key.

70. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 69, wherein the short-term key information is a random value.

71. (Previously Presented) A method for broadcasting encrypted multimedia content as defined in claim 64, wherein at least one terminal comprises a mobile station.

72. (Currently Amended) An integrated circuit for a mobile station, comprising:

means for forwarding a unique public key over the air to a content provider;

means for securely storing a unique private key, corresponding to the unique public key, such that the unique private key is not accessible to a user, wherein the means for securing storing has processing power sufficient to decrypt a broadcast access key and to generate a short term key, and does not have processing power sufficient to decrypt multimedia content, and wherein the content provider encrypts a broadcast access key with the unique public key to authorize an integrated circuit securely storing a corresponding unique private key to receive encrypted multimedia content;

means for receiving the respective encrypted broadcast access key over the air from the content provider;

means for decrypting the encrypted broadcast access key and securely storing the broadcast access key, wherein the securely stored broadcast access key is not accessible to a user;

means for receiving short-term key information and the encrypted multimedia content broadcast over the air from the content provider to a plurality of mobile stations, wherein the multimedia content is encrypted with a short-term key, and wherein the short-term key is generated using the broadcast access key and the short-term key information;

means for generating the short-term key using the securely stored broadcast access key and the broadcast short-term key information; and

means for decrypting the multimedia content using the short-term key, wherein the means for securely storing provides more secure key storage than the means for decrypting the multimedia content.

73. (Previously Presented) An integrated circuit as defined in claim 72, wherein the short-term key is accessible to a user.

74. (Previously Presented) An integrated circuit as defined in claim 72, wherein the short-term key information is the short-term key encrypted using the broadcast access key.

75. (Previously Presented) An integrated circuit as defined in claim 72, wherein the short-term key is generated by applying a cryptographic hash to a concatenation of the short-term key information and the broadcast access key.

76. (Previously Presented) An integrated circuit as defined in claim 75, wherein the short-term key information is a random value.

77. (Currently Amended) A machine readable medium, comprising:

code for forwarding a unique public key over the air to a content provider;

code for securely storing a unique private key, corresponding to the unique public key, in a secure processing unit of a terminal such that the private key is not accessible to a mobile equipment of the terminal ~~user~~, wherein the secure processing unit provides more secure key storage than the secure processing unit, wherein the secure processing unit has processing power sufficient to decrypt a broadcast access key and to generate a short term key, and does not have processing power sufficient to decrypt multimedia content, and wherein the ~~content provider encrypts a~~ broadcast access key is encrypted by the content provider using ~~with~~ the unique public keys of each of the respective terminals to authorize the respective [[a]] terminal ~~storing a corresponding unique private key~~ to receive encrypted multimedia content;

code for receiving the respective encrypted broadcast access key over the air from the content provider;

code for decrypting the encrypted broadcast access key and securely storing the broadcast access key, wherein the securely stored broadcast access key is not accessible to a user;

code for receiving short-term key information and the encrypted multimedia content broadcast over the air from the content provider to a plurality of terminals each having the

integrated circuit, wherein the multimedia content is encrypted with a short-term key, and wherein the short-term key is generated using the broadcast access key and the short-term key information;

code for generating the short-term key using the securely stored broadcast access key and the broadcast short-term key information; and

code for decrypting the multimedia content using the short-term key.

78. (Previously Presented) A machine readable medium as defined in claim 77, wherein the short-term key is accessible to a user.

79. (Previously Presented) A machine readable medium as defined in claim 77, wherein the short-term key information is the short-term key encrypted using the broadcast access key.

80. (Previously Presented) A machine readable medium as defined in claim 77, wherein the short-term key is generated by applying a cryptographic hash to a concatenation of the short-term key information and the broadcast access key.

81. (Previously Presented) A machine readable medium as defined in claim 80, wherein the short-term key information is a random value.

82. (Currently Amended) An apparatus for receiving encrypted multimedia content broadcast over the air from a content provider to a plurality of authorized apparatuses, comprising:

a mobile equipment configured to:

forward a unique public key over the air to the content provider, and

decrypt the multimedia content using a short-term key, wherein the multimedia content is encrypted with the short-term key, and wherein the short-term key is generated using a broadcast access key and short-term key information; and

a secure processing unit configured to:

securely store a unique private key, corresponding to the unique public key, such that the unique private key is not accessible to the mobile equipment ~~a user~~, wherein the secure processing unit provides more secure key storage than the secure processing unit, wherein the secure processing unit has processing power sufficient to decrypt a broadcast access key and to generate a short term key, and does not have processing power sufficient to decrypt multimedia content, and wherein the content provider encrypts the broadcast access key with the unique public key to authorize an apparatus having the secure processing unit securely storing the corresponding unique private key to receive the encrypted multimedia content;

receive the respective encrypted broadcast access key over the air from the content provider;

decrypt the encrypted broadcast access key and securely store the broadcast access key, wherein the securely stored broadcast access key is not accessible to a user;

receive the short-term key information broadcast over the air from the content provider to the plurality of apparatus;

~~generating~~ generate the short-term key using the securely stored broadcast access key and the broadcast short-term key information.

83. (Previously Presented) An apparatus as defined in claim 82, wherein the short-term key is accessible to a user.

84. (Previously Presented) An apparatus as defined in claim 82, wherein the short-term key information is the short-term key encrypted using the broadcast access key.

85. (Previously Presented) An apparatus as defined in claim 82, wherein the short-term key is generated by applying a cryptographic hash to a concatenation of the short-term key information and the broadcast access key.

86. (Previously Presented) An apparatus as defined in claim 85, wherein the short-term key information is a random value.